# 2. Xmas scans: turning network packets into holiday lights!

An `Xmas` scan utilizes TCP packets flagged with `FIN`, `PSH`, and `URG` to stealthily detect open ports, leveraging its unique packet configuration to potentially bypass firewall detection.

This technique, named for its `illuminated` packet headers, primarily receives responses from closed ports, making it a subtle tool for network analysis.

Write a bash script that executes a `xmas scan` on a test network.The scan should identify potential stealth ports, focusing on ports `440` to `450`.

- Your script should accept `host` as an arguments `$1`.
- Your script should only show open (or possibly open) ports.
- Your script should show all packets sent and received.
- Your script should display the reason each port is set to a specific state.

*Depending on the scanned network, the output could change.*

```
┌──(maroua)-[~/0x06_nmap_advanced_port_scans]
└─⚑  ./2-xmas_scan.sh www.holbertonschool.com
[sudo] password for maroua:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-18 15:54 CET
SENT (0.1584s) ICMP [10.5.202.26 > 52.17.119.105 Echo request
(type=8/code=0) id=40212 seq=0] IP [ttl=56 id=56105 iplen=28 ]
SENT (0.1584s) TCP 10.5.202.26:57513 > 52.17.119.105:443 S ttl=49 id=2579
iplen=44  seq=1688269977 win=1024
SENT (0.1584s) TCP 10.5.202.26:57513 > 52.17.119.105:80 A ttl=43 id=33442
iplen=40  seq=0 win=1024
SENT (0.1584s) ICMP [10.5.202.26 > 52.17.119.105 Timestamp request
(type=13/code=0) id=36086 seq=0 orig=0 recv=0 trans=0] IP [ttl=45 id=39982
iplen=40 ]
RCVD (0.2425s) TCP 52.17.119.105:443 > 10.5.202.26:57513 SA ttl=107 id=0
iplen=44  seq=960423197 win=62727
NSOCK INFO [0.2810s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.2810s] nsock_connect_udp(): UDP connection requested to
127.0.0.53:53 (IOD #1) EID 8
NSOCK INFO [0.2810s] nsock_read(): Read request from IOD #1 [127.0.0.53:53]
(timeout: -1ms) EID 18
NSOCK INFO [0.2810s] nsock_write(): Write request for 44 bytes to IOD #1 EID
```

```
27 [127.0.0.53:53]
NSOCK INFO [0.2810s] nsock_trace_handler_callback(): Callback: CONNECT
SUCCESS for EID 8 [127.0.0.53:53]
NSOCK INFO [0.2810s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS
for EID 27 [127.0.0.53:53]
NSOCK INFO [0.5500s] nsock_trace_handler_callback(): Callback: READ SUCCESS
for EID 18 [127.0.0.53:53] (107 bytes)
NSOCK INFO [0.5500s] nsock_read(): Read request from IOD #1 [127.0.0.53:53]
(timeout: -1ms) EID 34
NSOCK INFO [0.5500s] nsock_iod_delete(): nsock_iod_delete (IOD #1)

[...]

Nmap scan report for www.holbertonschool.com (52.17.119.105)
Host is up, received syn-ack ttl 107 (0.083s latency).
Other addresses for www.holbertonschool.com (not scanned): 34.249.200.254
63.35.51.142
rDNS record for 52.17.119.105: ec2-52-17-119-105.eu-west-
1.compute.amazonaws.com

PORT    STATE         SERVICE       REASON
440/tcp open|filtered sgcp          no-response
441/tcp open|filtered decvms-sysmgt no-response
442/tcp open|filtered cvc_hostd     no-response
443/tcp open|filtered https         no-response
444/tcp open|filtered snpp          no-response
445/tcp open|filtered microsoft-ds  no-response
446/tcp open|filtered ddm-rdb       no-response
447/tcp open|filtered ddm-dfm       no-response
448/tcp open|filtered ddm-ssl       no-response
449/tcp open|filtered as-servermap  no-response
450/tcp open|filtered tserver       no-response
```